**REPORT DOCUMENTATION PAGE**

| | |
|---|---|
| **1. Report Security Classification:** UNCLASSIFIED | |
| **2. Security Classification Authority:** | |
| **3. Declassification/Downgrading Schedule:** | |
| **4. Distribution/Availability of Report:** DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED. | |
| **5. Name of Performing Organization:** Dean of Academics Office | |
| **6. Office Symbol:** 1 | **7. Address:** NAVAL WAR COLLEGE<br>686 CUSHING ROAD<br>NEWPORT, RI 02841-1207 |
| **8. Title** (Include Security Classification): FOLLOW THE MONEY: USING COMPUTER NETWORK ATTACK TO ENFORCE ECONOMIC SANCTIONS | |
| **9. Personal Authors:** PAUL R. YOUNES LCDR USNR | |
| **10.Type of Report:** FINAL | **11. Date of Report:** 17MAY01 |
| **12.Page Count:** 21 | |
| **13.Supplementary Notation:** A paper submitted to the Dean of Academics, Naval War College, for the B. FRANKLIN REINAUER II DEFENSE ECONOMICS essay competition. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy. | |
| **14. Ten key words that relate to your paper:** ECONOMIC WARFARE SANCTIONS COMPUTER NETWORK ATTACK BANKING DIPLOMACY INTERNATIONAL LAW CONFLICT | |

**15.Abstract:**

ECONOMIC SANCTIONS HAVE PRODUCED MIXED RESULTS AS TOOLS OF POLITICAL AND DIPLOMATIC COERCION. DUE TO THE UNIQUE CHARACTERISTICS OF COUNTRIES RULED BY DICTATORS OR ELITES, SANCTIONS ARE OFTEN INEFFECTIVE. THE USE OF COMPUTER NETWORK ATTACK (CNA) COULD PROVIDE AN EFFECTIVE MEANS OF INFLUENCING DICTATORS. BY ATTACKING THEIR PERSONAL OR GOVERNMENTAL WEALTH, THEIR POLITICAL AND ECONOMIC INFLUENCE COULD BE DRASTICALLY REDUCED.

| | | |
|---|---|---|
| **16.Distribution / Availability of Abstract:** | **Unclassified** X | **Same As Rpt** |



| | |
|---|---|
| **17.Abstract Security Classification:** UNCLASSIFIED | |
| **18.Name of Responsible Individual:** Dean of Academics, Naval War College | |
| **19.Telephone:** 841-2245 | **20.Office Symbol:** 1 |

NAVAL WAR COLLEGE
Newport, R.I.

# Follow the Money

## Using Computer Network Attack to Enforce Economic Sanctions

By

Paul R. Younes

LCDR USNR

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of National Security Decision Making.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: 

17 May 2001

Economic power is the use of economic force by one nation against another to achieve a national objective.[1] Governments use economic sanctions as means of changing another government's policy without first going to war. However, economic coercion only works within a narrow set of constraints; anything outside these constraints produces relatively unsuccessful results. Computer Network Attack (CNA), if used in a strategic and specific manner, could provide a tool that would make the applications of economic force more effective against nations that the US desires to influence.

A "sender" country uses economic power against a "target" country for several reasons[2]: to punish a country for behaving badly, to prevent adversaries from getting certain categories of goods, or to induce another country to do something. Table 1[3] lists various instruments of economic force that one country could use against another.

[1] John C. Scharfen, The Dismal Battlefield (Annapolis: Naval Institute Press1995), 42.
[2] Speech by Ambassador Paul Taylor at the 1998 Current Strategy Forum, 16 June, 1998. Naval War College. Lkd. http://www.nwc.navy.mil/dsd/economic_coersion_in_the_service.htm.
[3] John C. Scharfen, The Dismal Battlefield (Annapolis: Naval Institute Press1995), 101.

Table 1 - Instruments of Economic Force

| TRADE | FINANCE | RESOURCE MANAGEMENT | UNCONVENTIONAL |
|---|---|---|---|
| Most-favored-nation status | Aid and loans | Stockpiling | Industrial Espionage |
| Boycott | Indebtedness | Autarky | Bribery |
| Sanctions | Withholding payments | Limited extraction | Disinformation |
| Blacklist/graylist | Freezing accounts | Preclusive purchasing | Inciting work stoppages |
| Export/import licensing | Nationalizing assets | Technology transfer | Immigration control |
| Export credit guarantees and insurance | Nationalizing assets | Resource denial | Disrupting lines of communication |
| International law | Impounding assets | | Computer subversion |
| Export and import embargoes | | | Currency subversion |
| Arms sales | | | Smuggling |
| Tariffs | | | Credit system subversion |
| Commodity dumping | | | Sabotage |
| Patent denial | | | Extortion |
| | | | Economic terrorism |
| | | | Economic propaganda |
| | | | Piracy |

Ironically, some forms of economic power, such as sanctions, are most effective against allies. Countries with similar political systems, and in which both countries benefit from commercial ties, have strong incentives to maintain good relations. While evidence suggests the form of government (democracy versus dictatorship) a target country has is unimportant in whether sanctions work[4], conflicts between competing ideologies and systems are highly visible and often involve issues of sovereignty and pride, which can prevent successful resolution of a conflict. Since the dissolution of the Soviet Union, the United States has increasingly tied the importance of democracy, human rights, and free markets to obtaining commercial trading privileges in the U.S. Consequently, the US seems to find itself in conflict more often with dictatorial governments who are more willing to begin and sustain hostilities, which include the use of military force.

These conflicts are taking place against the backdrop of a changing international economic system. Dr. Thomas Barnett uses a tiered model to describe three "perspectives" to analyze "interstate relations in the post-Cold War era..." [5]

- The individual perspective, from which a nation-state's citizens view their environment;
- The nation-state perspective, in which states interacts with other states;

---

[4] Daniel Drezner, "Serious About Sanctions," in Strategy and Force Planning, 3rd edition, ed. Strategy and Force Planning Faculty (Newport: Naval War College Press, 2000), 273.

[5] Thomas P.M. Barnett, "Life After DoDth or: How the Evernet Changes Everything," Proceedings, (May 2000): 48-53.

Thomas P.M. Barnett with Bradd C. Hayes, Asian Energy Futures: Decision Event Report I of the New Rules Sets.Project. (Newport: Center for Naval Warfare Studies – Decision Support Department, 2000) 5-8.

This model is an adaptation of a model presented in Kenneth Waltz's study, *Man, the State, and War* (New York: Columbia University Press).

- The international perspective, from which the globalized international system, increasingly defined by non-governmental organizations and operating outside the parameters of the individual states, allocates resources and power.

Barnett notes that within the context of this model,

> ...the United States has not yet adjusted its state-centered defense policy to account for the two biggest security trends of the globalization era:
>
> - Power and competition have shifted upward, from the state to the system (in the form of the global economy, culture, and communications grid).
> - Violence and defense spending (e.g., small arms races, private security firms) have shifted downward, from the state to the individual. [6]

This same observation also provides a partial explanation for the failure of traditional economic force to influence nation-state behavior. For example, nations such as Iraq or Cuba can interact with a globalized economy to take advantage of leakage in the sanctions regime to bolster their economy. Furthermore, those who hold power at the nation-state level can regulate the commercial benefits to sustain and strengthen their regime, while depriving individuals of any benefit.

The U.S. government's attempts to use sanctions against adversarial countries, such as Cuba, Iraq, North Korea, and Panama, have often failed, and in two of these cases ended in military action. The U.S. imposed sanctions on these governments, as well as others, to destabilize the existing government, and bring in new players that would be more amenable

[6] Ibid.

to U.S. guidance. Since 1918,the U.S. has used sanctions fifteen times in an attempt to destabilize a target government.[7] Six of these countries were governed by dictatorships.

The US government assumes that by imposing economic sanctions against a country with a dictatorial government, the people will grow weary of economic deprivation and revolt against the "trouble-making elites"[8] or dictator, and replace them with a different government. This assumption has repeatedly been discredited. In fact, economic pain imposed on a country has had two different effects. If the people support the dictatorship, their resolve is frequently stiffened, often because of the excellent propaganda that blames the United States for the country's deteriorating condition. This result is observable in Cuba, Iraq, and to a lesser degree, Nicaragua.

The other effect is a shifting of economic and social pain down from the nation-state to the individual level. Dictators frequently move the economic pain of sanctions to those who have no political voice are thus frequently insulated from its effects. A dictator's political and military allies are also spared, and often enriched, during the imposition of sanctions. The people of the target country, however, are usually unable to even get necessities. For instance, in Iraq, Saddam Hussein's " use of terror, rewards, and nationalistic sentiments enable his regime to rise above any opposition. He has easily won loyalty by providing jobs and other benefits to the estimated 1 million members and supporters of the ruling Baath Party."[9]

---

[7] Gary Clyde Hugbauer, Jeffrey J. Schott, and Kimberly Ann Elliot, Economic Sanctions Reconsidered, 2nd ed. (Washington D.C.: Institute for International Economics, 1990,) 59. This source lists 14; I have added the case of US v. Iraq.

[8] Chantal de Jonge Oudraat, "Making Economic Sanctions Work," Survival, 42 (Autumn 2000): 105.

[9] LTCOL Douglas C. Bonner, Making Economic Sanctions An Effective Alternative. (Carlisle Barracks, PA: U.S. Army War College) 24.

Simultaneously, Hussein shifted the economic pain of U.N sanctions to the Kurds and Shia Muslims in his country, citizens who had little influence in Iraq's politics. He has punished them for their short-lived rebellions by denying them electricity, food, goods and services, while simultaneously attacking them militarily.[10]

Haiti and Panama provide further examples. In both cases, the people who suffered the most from sanctions had no political influence over their authoritarian government, and thus were unable to effect any change. In Panama, General Noriega established himself as part of a military government, and disestablished the Panamanian congress. Similarly, the Haitian military actually gained influence during the U.S. led embargo, since it controlled many of the economic resources. The poor in Haiti, most of whom supported Aristide, had no influence over the political process.

This U.S. policy fails because it underestimates the political power wielded by dictatorships. Dictators can use domestic police and security forces against their own populace, while wielding the shield of national sovereignty to protect themselves internationally. Any credible or viable political opposition that could rally the country to a revolt has already been eliminated, or driven underground.

In addition, the use of economic sanctions by the U.S. is rarely used as part of a coherent strategy, or an appreciation of how to best use economic tools as a means of obtaining political or diplomatic concessions. Potential solutions to disagreements between states can range from diplomatic and political initiatives, to economic sanctions, to the use of military force. However, U.S. leaders do not view sanctions as part of a continuum of force.

[10] Taylor speech.

The government's imposition of sanctions is often the sole response to a situation, not as part of either a cohesive political, diplomatic, or military effort[11] (Taylor), and with little thought given to potential follow-on actions.

Furthermore, while the desired goals of economic force are often well articulated, the strategy to obtain them is not. U.S. policy makers often view the imposition of sanctions as *the* strategy, not as part of an *overall* strategy. The desire to take, or appear to take, firm action often motivates policymakers to impose economic measures.[12] Short of using military force, cutting economic ties seems to be the surest way to express disapproval of the target country.

In addition, globalization has weakened the effectiveness of economic actions, especially unilateral ones. Severed economic ties between the sending and target country are often quickly built again with other countries, who are motivated either by the desire to do more business with the target country, or to spite the country imposing the economic force. Frequently, rerouting goods and smuggling can fill the needs of the target country.[13]

The question for policy makers then becomes: How can countries, such as the U.S., use economic power to make hostile, rogue, dictators feel enough economic pain to alter their course of action? Or, to re-phrase the question using Barnett's three-tiered model, how can a sending country impose economic violence at the individual level against dictators who hide behind a nation-state structure?

---

[11] Ibid.

[12] Douglas Johnston and Sidney Weintraub, Altering U.S. Sanctions Policy (Washington DC: CSIS, 1999).

Ernest Preeg, Feeling Good or Doing Good With Sanctions, (Washington DC: CSIS, 1999).

[13] Scharfen, 96

First, as with any initiative, decision makers contemplating economic warfare must develop a clear strategy for obtaining the desired results. Ambassador Paul Taylor developed criteria for conducting economic warfare based on his reading of von Clausewitz' *On War*[14]. They include:

- Support within the U.S populace. Depending on the circumstances, obtaining popular support might be difficult. The U.S. business community lobbied strongly for normalized trade relations with China, despite evidence of human rights violations, and charges of espionage efforts against both public and commercial institutions in the U.S.

- Determining the degree to which an adversary is susceptible to this kind of pressure. Iraq, Panama, and Haiti provide examples of circumstances where dictators are, or were, not affected by the economic pain of the people, or any political pressure they could potentially exert.

- Determining who in the target country will be hurt by economic sanctions, and whether they have the political influence to make the government accept our demands. In short, the U.S. must specifically identify decision makers on whom the exertion of painful pressure will make a difference in the target country's policy.

- The willingness of other countries to cooperate with us. Leakage in a sanctions regime can undercut both the purpose of the sanctions, and the credibility of the nation's imposing the sanctions. For example, oil smuggled from Iraq through the

[14] Taylor speech.

Turkish and Syrian borders contributes approximately $14 million a day to the Iraqi government, outside of U.N. controls.[15]

- The overall adequacy of the sanctions strategy to achieve the sought-after objective.

- Whether we are willing to go to armed conflict to reach our objective if sanctions fail.

Given the ineffectiveness of traditional uses of economic force to make dictators more compliant, the US should use computer network attack (CNA), in conjunction with other policy tools, to attack the economic institutions and resources that provide wealth to dictators, as a subset of economic sanctions. CNA, classified as an "unconventional" or asymmetric instrument, could become an effective weapon and potential deterrent to dictators. Sanctions, blockades, and other economic measures frequently do not work because the decision-makers are insulated from the effects. In searching for a means of inflicting targeted pain, CNA is an excellent weapon.

The ambiguity in international law as to whether a CNA constitutes an attack in the classic military sense gives the decision makers of the sending country some latitude in the use of CNA. Much depends on how the international community perceives the motives for the attack, the means of attack, and the results. A Department of Defense assessment of international legal issues involved in information operations stated that,"...the consequences are likely to be more important than the means used."[16]

---

[15] Jessica Barry, "Iraqis Step Up Secret Russian Weapons Trade," London Sunday Telegraph, 25 February, 2001, Lkd. <http://ebird.dtic.mil> [25 February, 2001].

[16] Department of Defense Office of General Counsel, An Assessment of International Legal Issues in Information Operations, May 1999. Lkd. <http://www.infowar.com/info_ops/DOD-IO-legal.doc>, [03 April 2001] pg. 18.

During a war, combatant forces are not supposed to target civilians, although collateral damage is acceptable if a target is considered highly important to the overall military objective. However, in conflicts from WWI on, military actions have increasingly affected civilians, yet few strategists (except perhaps on the losing side) disputed the need to destroy key economic activities, such as aircraft manufacturing plants, oil refineries, and other industrial activities. However, when using economic power, civilian casualties must be anticipated as a consequence of the policy; indeed, it is the economic pain of the civilian population that is expected to reach the government and force the government to do the U.S. will.

CNA should complement the use of economic instruments by pinpointing economic and financial repositories of wealth that provide political power to decision-makers in the target country. What makes CNA an especially effective weapon is that it can discriminate between specific targets. CNA against an individual or an institution will not necessarily cause the same type of collateral damage (social, economic, structural) that frequently accompanies the use of sanctions or blockades. The U.S. can use CNA against specific nodes, rather than an entire system or country.

For instance, the contents of individual bank accounts, both foreign and domestic, of a country's government and business leaders could be emptied or transferred. The U.S. allegedly targeted Slobodan Milosevich's bank accounts during the NATO bombing campaign, although high-level defense department sources have stated that the U.S. did not penetrate any banking networks;[17] "The mission was reputedly overseen by the Joint Chiefs

[17] William Arkin, "The Cyber-Bomb in Yugoslavia," Washington post.com, 25 October, 1999.

of Staff (JCS)- managed [by the] Information Operations Technology Center (IOTC) housed at the NSA."[18] Government accounts used for the purchase of military supplies could also be deleted or transferred.[19] In one alleged incident during the 1990's, the CIA remotely deleted a drug lord's bribe to a corrupt South American government official from a bank's records. The disappearance of the money led to confusion and recriminations, and resulted in the execution of a bookkeeper.[20]

Businesses operated as a means of funding terrorist organizations or governments could be especially vulnerable to CNA. The East Africa Embassy bombings trial revealed the extensive business organization Osama Bin Laden used to assist in financing his terrorist activities. An international corporate group called Al Qaeda (Arabic for the Base) was instrumental in organizing and financing terrrorist activities, according to testimony from Jamal Ahmend Al-Fadl, the former paymaster.[21] According to Al-Fadl, Al Qaeda was a corporate shell that operated out of the Sudan. Under its corporate umbrella, an import-export concern, a currency trading concern, a road construction firm, a farm, and a newspaper, provided revenue to the parent organization. Bank accounts were kept in financial institutions in the Sudan, Malaysia, Britain, Hong Kong, and Dubai. More recently, one newspaper revealed Bin Laden also maintains accounts in Cyprus, where money from his Sudanese

---

[18] Anthony Kimery, "The Army As Digital Defender," Military Information Technology, Vol. 4, No. 2. Lkd. <http://www.mit-kmi.com/Archives/4_2_MIT/4_2_Art1/cfm> [3 April, 2001]. Pg 2-3.

[19] "US military prepares for Information War against Yugoslavia." War in the Balkans. 08 May 1999. Lkd. <http://www.informationwar.org/_balkans/00000028.htm> [03 April 2001].

[20] Ibid.

[21] Alan Feuer, "Jihad Inc Finds a Business in Terrorism," New York Times 13 February 2001, Lkd. http://ebird.dtic.mil [13 February, 2001].

Benjamin Weiser, "Ex-Aide to Bin Laden Describes Terror Campaign Aimed At U.S.," New York Times 07 February 2001, Lkd. <http://ebird.dtic.mil> [07 February, 2001].

business operations are deposited.[22] The earnings from these businesses funded travel, arms purchases, and training areas.

Saddam Hussein provides another example of how conventional economic sanctions are failing to achieve stated objectives, and where CNA could prove effective. Under the supervision of the United Nations, Iraq has been selling oil, payment for which is transferred into a special escrow account that is specifically designed to buy food, medicine, and consumer goods for the Iraqi people. However, Hussein is also smuggling oil out of Iraq through a Syrian pipeline, with trucks over the Turkish border, and, with Iranian assistance, with ships out through the Persian Gulf, for which he is receiving full payment. One estimate places Saddam's earning from the illegal oil at approximately $1 billion annually. The establishment of this illegal "slush" fund assists Hussein in maintaining power, and provides money for rearming the military, rebuilding his Weapons of Mass Destruction (WMD) capability, and providing favors for political allies.[23]

Using CNA to target the accounts with which Hussein buys arms and gives favors would remove a large part of his power base. Without funding for B'aath Party supporters, or weapons programs, Hussein would lose political influence.

Like Osama bin Laden, the Chinese army used commercial activities to fund its growth and operations. Until 1998, the Chinese Army was involved in manufacturing, import-export, smuggling, hotels management, and at one point, opium smuggling. In 1998, after several smuggling scandals, China's civilian leadership told the PLA to divest itself of

[22] "Bin Laden maintains accounts in Cyprus," World Tribune.com, 10 April, 2001.
[23] Gerald Seib, "Bush's Key In Curbing Iraq: Follow The Money," Wall Street Journal, 21 February 2001, Lkd. <http://ebird.dtic.mil> [21 February, 2001].

commercial activities, with the exception of telecommunications. [24] However, the Federal Bureau of Investigation (FBI) has

> ...compiled a list of more than 3,000 Chinese government-linked businesses operating in the United States. The FBI's counterspies say at least 300 of the Chinese entities not only fund Beijing's military but are used to provide cover for intelligence officers or intelligence-gathering activities.[25]

Most analyses focus on the use of CNA as an extension of military force, and apply international law using the customary rules of warfare. However, an advantage of using CNA as a weapon of *economic* force is that legal considerations regarding the use of CNA as a weapon of military conflict can be sidestepped, when applied to either individuals or governments. As one author noted, "...the customary usage of economic force...validate the rights of the state to use the economic instrument coercively for the good of a single nation or the world in general."[26] In addition, there "are no laws that could be considered a code of conduct for the prosecution of an economic conflict."[27] Laws governing military warfare require "discrimination norms for the use of military force [that] specifically prohibit targeting civilian populations. There are serious problems in associating this norm with the use of economic force."[28]

The U.S. could use CNA to attack larger targets. Central banks, currency exchanges, currency manipulation, or rumors spread about the economic health of a country could lead to economic disruption. However, the risks for attacking these larger targets in a globalized economic system are greater. There could be unforeseen effects after a CNA against a target

---

[24] Jim Mann, "Is China Army Going Out Of Business," Los Angeles Times, 21 February, 2001, Lkd. <http://ebird.dtic.mil> [21 February, 2001].
[25] Bill Gertz and Rowan Scarborough, "Inside The Ring," Washington Times, 9 February, 2001, Lkd. <http://ebird.dtic.mil> [21 February, 2001].
[26] Scharfen, 86.

country's infrastructure. While an attack against individual or even some limited government accounts would not cause widespread disruption, moving against a target country's banks or exchanges could upset established economic equilibrium with other countries bound financially, economically, or commercially. In addition, there is no way to predict how quickly economic equilibrium could be restored. During an economic security exercise held at the Naval War College, political instability in Asia, coupled with CNA, caused increases in oil prices, gold prices, a decrease in the value of the yen against the dollar, a drop in the Dow-Jones Industrial Average and Nikkei, and in decrease in bond yields, indicating increased sales of bonds.[29] The exercise did not attempt to predict how long the effects from the CNA would last.

There is substantial risk in using CNA as a weapon. Other countries may learn from our techniques, and follow our example. Given the legal uncertainties that surround CNA, the US may provide precedent for other countries to use similar attacks against the U.S.

The implementation of this policy would require several decisions. The U.S. would need to determine, on a case-by-case basis, if the attacks should be publicized. The use of CNA as a covert weapon would not necessarily diminish its effectiveness. The targeted leaders and organizations would certainly know that something occurred. Furthermore, the confusion and fear caused by seeing a bank account emptied could provide an important psychological advantage. Any public complaint could expose the extent of the dictator's financial assets, and expose self-interest. A dictator may be tempted to risk war for an

---

[27] Scharfen, 95.
[28] Scharfen, 92.
[29] Naval War College Intranet Lkd. <http://ncwintranet/dsd/ese1> & <http://ncwintranet/dsd/ese2>, 24.

economy, but would have a harder time justifying a country's suffering while he is still profiting.

The U.S. may not want other nations to know its capabilities and expertise with this form of attack. CNA is difficult to trace at this time, and while some technology is making it easier to find the origin of attacks, other technology is making it more difficult. Maintaining deniability may be important for public relations.

Superior economic and human intelligence would also be required. The U.S. would need to conduct intelligence gathering on both hostile and friendly networks on a constant basis. Computer network tools that can enter both hostile and friendly networks would also be required. Obtaining financial intelligence from police forces and financial institutions would assist in locating "accounts of interest." However, this cooperation is not essential. Banks are a frequent, and sometimes easy, target for hackers intent on theft.[30]

More difficult than exercising CNA technology will be the development of effective policy guidance. At present, no central coordinating agency or individual exists that develops or coordinates economic force strategy, makes recommendations to the National Command Authority; only the Office of Foreign Assets Control monitors sanctions effects, although under the new Bush Administration, the National Security Council appears to be preparing to emphasize the economic aspects of national security.[31] Greater US interagency cooperation would be required between organizations such as the Departments of the Treasury, Commerce, Justice, and Defense. The civilian branches of government have largely

---

[30] Michelle Delio, "Brit Cops Tackle E-Thievery," Lkd. Wired News,19 April, 2001. <http://www.wired.com/news/business/0,1367,43171,00.html?tw=20010421> [21 April, 2001].

concentrated on Computer Network Defense (CND). The Army and Air Force are developing expertise in this area, while U.S SPACECOM was recently assigned responsibility for computer network defense and attack, and designated a Joint Task Force-CND and CNA. The CIA, NSA, and Federal Reserve, National Security Council and National Economic Council would also need to be involved.

The question of who would conduct CNA is complicated by the traditional U.S. hostility to giving military forces any tools that could be used against its own citizens. Foreign governments, police forces, and financial institutions would most likely mirror this suspicion if the DoD attempted to obtain information from them on their citizens, or used their networks to conduct CNA operations. CNA necessarily takes place largely over civilian networks. This would imply that civilian agencies would conduct CNA. However, the application of economic force involves actions directed towards foreign countries, which falls under the authority of the Department of State and Defense. At this time, the military has authority to respond to attacks on military systems, although an all-out response to intrusions is rare.[32] Civilian law enforcement agencies, such as the FBI's National Infrastructure Protection Center, monitor civilian networks.

Presently, the authority to conduct CNA, such as the attacks against Serbian air defense computers during the Operation Noble Cause, requires presidential authority, much as the decision to deploy Weapons of Mass Destruction (WMD). The level of decision-making should correspond to the potential consequences of the attack; the use of economic

---

[31] Karen DeYoung and Steven Mufson, "Leaner, Less Visible NSC Taking Shape," Washington Post, 10 February, 2001, Lkd. http://ebird.dtic.mil [10 February, 2001].
[32] Vernon Loeb, "Pentagon Computers Under Assualt," Washington Post, 7 May,2001, Lkd. <http://ebird.dtic.mil> [7 May, 2001].

force, including the use of CNA, is a strategic issue, and decision-making should be kept at high levels.

The interagency nature of CNA will complicate this process. The special nature of this technology makes large command structures unnecessary; a President could tell one government computer expert when and what to do. The purpose of everyone else involved in the decision is to explore and assess the complicated policy issues inherent in using a new weapon.

These efforts may be further along than is often suspected. President Ronald Reagan, at the behest of NSC and CIA officials, allegedly gave permission "to penetrate the computer infrastructures of financial institutions, foreign intelligence agencies, terrorist organizations and drug cartels worldwide...principally via bugged hardware and software sold by front companies run by the CIA and the National Security Agency..."[33]

CNA is, and will continue to be, a unique weapon of force. The "Wild West" aspect of CNA raises many questions about its deployment. It has the potential to precisely discriminate between targets, giving the U.S. the capability to conduct initially precise operations. As long as the target is well-defined, CNA could be an effective weapon. However, the aftereffects of conducting a less-defined CNA are potentially indiscriminate and broad, possibly ending in messy results. Like the use of any other weapon system, the technology will not substitute for precise strategy, and a clear formulation by decision makers on what they are attempting to accomplish.

---

[33] Anthony Kimery, "The Army As Digital Defender," Military Information Technology, Vol. 4, No. 2. Lkd. <http://www.mit-kmi.com/Archives/4_2_MIT/4_2_Art1/cfm> [3 April, 2001]. Pg 2.

## BIBLIOGRAPHY


Bayles, William J. Moral and Ethical Considerations for Computer Network Attack as a Means of National Power In Time of War, Chairman of the Joint Chiefs of Staff Strategy Essay Competition: Essays 2000. Washington DC: National Defense University, 2000.

Bonner, Douglas C. Making Economic Sanctions An Effective Alternative. Carlisle Barracks, PA: DTIC/U.S. Army War College, 1999.

Cebrowski, A.K. "CNE And CNA In The Network Centric Battlespace; Challenges For Operators And Lawyers." Speech. U.S. Naval War College Symposium, Newport, RI: 22 June 1999. <http://wwww.nwc.navy.mil/pres Speeches/computer%20Network%20Attack%20Speech.htm>

Center For Strategic and International Studies. Altering U.S. Sanctions Policy. Washington, DC: 1999.

Chritchlow, Robert D. "Whom the Gods Would Destroy: An Information Warfare Alternative for Deterrence and Compellence." Naval War College Review, 53 (Summer 2000): 21-38.

Congressional Budget Office. The Domestic Costs of Sanctions On Foreign Commerce. Washington DC: 1999.

Cook, Nick. "Brain Storming," Jane's Defence Weekly, 34 (23 August 2000): 28-32.

Department of Defense Office of General Counsel. An Assessment of International Legal Issues In Information Operations. May 1999. <http://www. Infowar.com/info_ops/DOD-IO-legal.doc> [3 April 2001].

Doran, George T. The Futility Of Economic Sanctions As An Instrument Of National Power In The 21st Century. Carlisle Barracks, PA: DTIC/U.S. Army War College, 1998.

Greenberg, Lawrence T., Seymour E. Goodman, and Kevin J. Soo Hoo. Information Warfare and International Law. Washington DC: National Defense University/DoD Command

and Control Research Program,1998.

Grove, Gregory D., Seymour E. Goodman and Stephen J. Lukasik. "Cyber-Attacks and International Law." Survival, 42 (Autumn 2000): 89-103.

Hayes, Bradd C. The Critical Link: Financial Implications Of National Security Threats. A Report of Economic Economic Security Exercise II 01 June 1998. <http:nwcintranet/dsd/Ese2.htm.[10 April 2001].

Hufbauer, Gary Clyde. "Sanctions-Happy USA." July 1998. International Economic Policy Briefs. Lkd. <http://www.iie.com/policybriefs/news98-4.htm> [23 April, 2001]. Reprinted from The Washington Post, Outlook section, 12 July 1998.

Hufbauer, Gary Clyde, Jeffrey J. Schott, and Kimberly Ann Elliott. Economic Sanctions Reconsidered: History And Current Policy, 2nd edition. Washington DC: Institute for International Economics, 1990.

Johnson, Jeffrey L. Economic Sanctions: Effectiveness As A Foreign Policy Tool In The Case Of The Former Yugoslavia. Monterey, CA: DTIC/Naval Postgraduate School, 1998.

Jonge Oudraat, Chantal de. "Making Economic Sanctions Work." Survival, 42 (Autumn 2000): 105-127.

Kimery, Anthony. "The Army As Digital Defender." Military Information Technology, Vol. 4, Issue 2, 2000. <http://www.mit-kmi.com/Archives/4_2_MIT/4_2_Art1.cfm>

Preeg, Ernest H. Feeling Good Or Doing Good With Sanctions. Washington, DC: Center For Strategic and International Studies, 1999.

Sands, Jeffrey I. Report On The Economic Security Exercise 24-25 October, 1997. <http://nwcintranet/dsd/ese1/htm> [10 April 2001].

Scharfen, John C. The Dismal Battlefield. Annapolis, MD: Naval Institute Press, 1995.

Sperber, JoAnn. "Strategic Partner: Providing DoD with World Class Information Systems." Military Information Technology, Vol. 4, Issue 6, 2000: 32-38.

Taylor, Paul. D. "Economic Coercion In The Service Of National Security." U.S. Naval War College Current Forum, Newport, RI: 16 June 1998. <http://www.nwc.navy.mil/dsd/economic_coercion_in_the_service.htm>.